|  |
| --- |
| **Facilitator Name: James Metzler** |
| Table Topic: Architecting Digital Environments to Enable Tailorable Shared Access (Industry and Gov Environments) |
|  |
|  |

Participants (spelled phonetically)

1. James Metzler, Lead Integrator, Digital Acceleration Task Force, working Enterprise Digital Environments
2. Westin Dudley, NG, AMT, integrating with ecosystems
3. Paul Nelson, NG, Leading DT for NGC Space Systems group (15k engineers); previously built cloud env
4. Rand Langmeed, Fellow at Siemens, working digital proving ground
5. Long Git, Dassault systems
6. Layla Akalon, Human Factors, Mile 2,
7. Alberto Ferrair, RTX, accelerating digital transformation in RTX (EN, ops, sustainment)
8. Jack Goodwyn, Stell, startup developing Requirements Mgmt Tool (alternate to DOORS), working AF ATO
9. Sybil Cambell, BAH, cloud arch SME, chief arch for LCMP with F-35
10. Chris Newbi, Director enterprise systems at BAH, Cross domain, working DAC

1. How can industry and government partners work together to establish common security standards and requirements for a shared digital environment?

* There are always challenges in handling new technologies, and common authentication is “a beast” of a challenge
* CAC is most widely used for government, but ECA and Yubikey are also possible
  + ECA is a good common option, but it needs to be implemented consistently at the DOD level
* Industry has the ability to allow Government/Customer access, but are generally unique, company-specific solutions
* Allowing access requires a balance with security partitioning
* Shared access also requires other organizations to pass trust down to sub-contractors and other participants
* ATOs are a challenge
  + The process needs to be standardized so it's not a new/unique process each time a company needs to do it
  + The current process is inconsistent across Bases and Services; shared reciprocity would be better
* There should also be parity in processes and authentication among security levels
  + A best practice is to keep the process at the lowest security level so others can see the full process without needing to be read in
* Shared access also presents a challenge with providing customers access to tools as large numbers might impact licensing amounts and contractors essentially funding licenses for stakeholders.

1. What are the implications of implementing a Zero Trust security model in a shared digital environment, and how can it be effectively implemented?

* Each application has to support all the layers of ZT; difficult to get non-cloud native vendors to adopt
* FIPS-14-3 Implementation important for vendors
  + Related to CMCC which is difficult for small companies
* ZT requires environment providers to become responsible for any tool on their system
* Have to drive vendors to SAML support; key consideration for startups and new architectures

1. How can continuous monitoring and vulnerability assessment be integrated into a shared digital environment to ensure ongoing security?

* There are requirements that come along with ZT
* Lots of tools are just logging everything, including irrelevant data, rather than specific user or security logs that would, for instance, allow one to to track what changed or what was accessed by a specific unauthorized user

Additional Discussion

* CSPs have key management and other services that can be leveraged
* AI may help in security monitoring and evaluation
  + E.g. some platforms have an ATO pipeline that is running checks along the ATO process
* Should shared Digital Environments be Gov or Industry hosted, or should ‘services’ be shared?
  + Sharing services raises continuous monitoring issues
  + TWC auto syncs for example have different implications
* The need for the environment can differ based on type of program (e.g. long sustainment chain)
* Shared infrastructure needs to protect IP
* Precise access control drives administrative costs
  + The tradeoff is often over classification (mark everything instead of delineating)
  + Culture needs to be in place to keep data at the lowest level possible

2. How can Industry and Government partners balance the need for standardization with the need for flexibility and innovation in software tool selection?

1. How can Industry and Government partners ensure that software versions used in collaborative reviews are compatible with each other and with existing systems?

* Tools are customized by users themselves, causing issues even among the same versions of tools
* At a higher level, compatibility about compliance with standards, not just the tools
* This also includes style guides, ontologies, naming, etc.
* Some applicable standards include:
  + By function ReqIF, SysML, Modeling language standard

1. Should Industry or Government be the driving force behind selecting software tools for collaborative reviews, and why?
2. How can Industry and Government partners ensure that software tools selected for collaborative reviews meet the necessary security, functionality, and usability requirements?
3. How can Industry and Government partners ensure that software tools are compatible with each other and with existing systems, even as new versions are released?